Method and device for verifying a file

Patent number: DE19961838

Publication date: 2001-07-05

Inventor: HEINS KERSTEN W (DE)

Applicant: SCM MICROSYSTEMS GMBH (DE)

Classification:

- international: H04L9/32; H04L9/30

- european: G06F1/00N1V2, G06F21/00N9C

Application number: DE19991061838 19991221

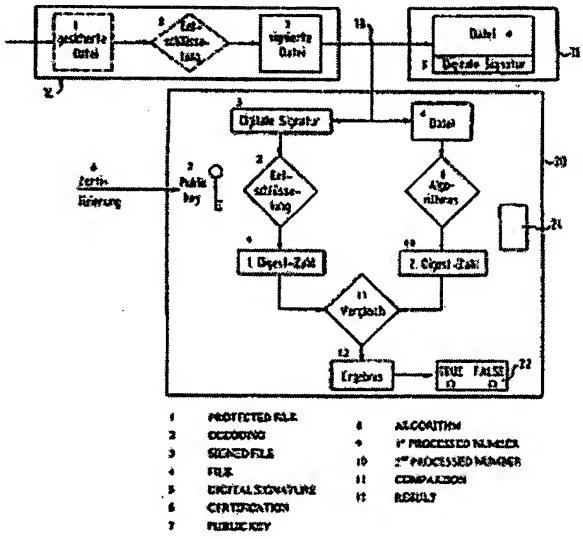
Priority number(s): DE19991061838 19991221

Also published as:

W O0146785 (A3)
W O0146785 (A2)
US 2003140229 (A1)

Abstract of **DE19961838**

The invention relates to a method and a device for verifying the authenticity and integrity of a file which has been received, or is to be transmitted from a computer (14) and which is furnished with a digital signature. For the verification process, said method accesses signals which are available at an interface (18) of the computer that is linked to an output device (16) for outputting the file furnished with the digital signature. A device (20) for carrying out the method comprises a circuit and a programme which are used to perform the verification in the device (20), in a manner which is logically separate from the central calculation unit of the computer (14). The device (20) is coupled to an interface (18) of the computer (14) that is linked to an output device (16), in such a way that it detects the signals used for the verification, in order to output the file furnished with the digital signature.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 61 838 A 1**

(51) Int. Cl.[7]: **H 04 L 9/32**
H 04 L 9/30

(21) Aktenzeichen: 199 61 838.0
(22) Anmeldetag: 21. 12. 1999
(43) Offenlegungstag: 5. 7. 2001

DE 199 61 838 A 1

(71) Anmelder:
SCM Microsystems GmbH, 85276 Pfaffenhofen, DE

(74) Vertreter:
Prinz und Partner GbR, 81241 München

(72) Erfinder:
Heins, Kersten W., 85354 Freising, DE

(56) Entgegenhaltungen:

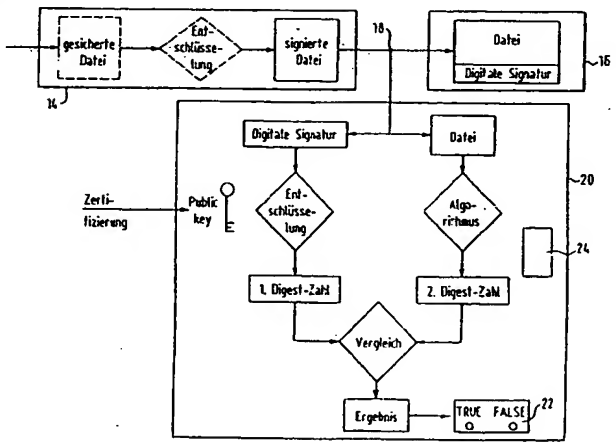
DE	195 32 617 C2
US	57 48 738
US	56 80 455
US	56 25 693
US	55 24 052
US	54 06 624
JP	09-3 11 854 A

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Vorrichtung zur Überprüfung einer Datei

(57) Ein Verfahren zur Überprüfung der Authentizität und Integrität einer von einem Rechner (14) empfangenen oder zu versendenden Datei, die mit einer digitalen Signatur versehen ist, greift zur Überprüfung auf Signale zu, die an einer Schnittstelle (18) des Rechners zu einem Ausgabegerät (16) für die Ausgabe der mit der digitalen Signatur versehenen Datei vorliegen. Eine Vorrichtung (20) zur Durchführung des Verfahrens umfaßt eine Schaltung und ein Programm, mit denen in der Vorrichtung (20) und logisch getrennt von der zentralen Recheneinheit des Rechners (14) die Überprüfung durchgeführt wird, wobei die Vorrichtung (20) mit einer Schnittstelle (18) des Rechners (14) zu einem Ausgabegerät (16) so gekoppelt ist, daß sie die für die Überprüfung verwendeten Signale zur Ausgabe der mit der digitalen Signatur versehenen Datei erfaßt.



DE 199 61 838 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur Überprüfung der Authentizität und Integrität einer von einem Rechner empfangenen oder zu versendenden Datei, die mit einer digitalen Signatur versehen ist. Die Erfindung betrifft ferner eine Vorrichtung zur Durchführung des Verfahrens.

Das Versenden und Empfangen von Dateien auf elektronischem Wege hat mit der fortschreitenden Entwicklung des Internet enorm an Bedeutung gewonnen. Gerade beim Austausch wichtiger Daten (sensitive data), wie er beispielsweise beim Handel über das Internet (e-commerce) stattfindet, besteht der Bedarf der Gewährleistung einer sicheren Datenübertragung. Dies resultiert aus der Tatsache, daß die Informationen, die über das Internet von einem Rechner zu einem entfernten anderen Rechner geschickt werden, eine Reihe von zwischengeschalteten Rechnern und separaten Netzwerken durchlaufen, bevor sie ihr Ziel erreichen. Somit besteht die Gefahr, daß die Übertragung der Daten mittels Dateien vor deren Empfang sowohl durch Übertragungsfehler als auch von dritter Seite auf unerwünschte Weise gestört werden kann.

Insbesondere der Empfänger einer übertragenen Datei hat ein Interesse daran, die Authentizität und die Integrität der empfangenen Datei überprüft zu wissen. Authentizität bedeutet in diesem Zusammenhang die Garantie, daß die Datei tatsächlich von der Person (oder von dem Unternehmen, etc.) stammt, die sich als Absender der Datei ausgibt. Die Integrität einer Datei ist gegeben, wenn deren Inhalt während der Übertragung nicht – vorsätzlich oder zufällig – verändert wurde. Bei bestimmten Anwendungen bestehen seitens des Empfängers die zusätzlichen Forderungen, daß die Vertraulichkeit der übertragenen Daten gewährleistet und/oder das Abstreiten des Versendens der Daten durch den Absender ausgeschlossen ist.

Die Sicherung der Datenübertragung unter Berücksichtigung der oben aufgeführten Aspekte erfolgt auf bekannte Weise unter Verwendung etablierter Techniken und Standards, die international akzeptiert sind und als Public-Key-Kryptographie bezeichnet werden. Ein wesentlicher Aspekt dieses Verfahrens ist das Versehen einer zu versendenden Datei mit einer digitalen Signatur, die nach dem Empfang der "signierten" Datei auf dem Rechner des Empfängers überprüft wird. Unter einer signierten Datei ist also in diesem Zusammenhang eine Datei samt ihrer zugehörigen digitalen Signatur zu verstehen.

Bei der Überprüfung besteht jedoch die Gefahr, daß bestimmte Viren oder andere bösartige Programme (z. B. spezielle Java-, ActiveX-Anwendungen, etc.) auf dem Rechner des Empfängers die Vorgänge der Überprüfung stören oder so beeinflussen, daß der Empfänger nicht bemerkt, daß die auf dem Bildschirm seines Rechners ausgegebenen Daten nicht mit den abgesandten Daten übereinstimmen. Andererseits ist es auch möglich, daß die Überprüfung der empfangenen Daten korrekt erfolgt und korrekt zu einem positiven Ergebnis führt, daß aber auf dem Bildschirm manipulierte Daten ausgegeben werden, ohne daß eine Warnung an den Empfänger erfolgt.

Das umgekehrte Problem kann auf der Seite des Absenders der Datei auftreten. Wenn beim Signieren einer zu versendenden Datei eine für den Absender nicht erkennbare Störung durch einen Virus oder dergleichen erfolgt, hat der Absender nicht die Möglichkeit, anhand der auf dem Bildschirm angezeigten signierten Datei den Fehler zu erkennen, insbesondere dann, wenn ein Fehler in der digitalen Signatur vorliegt.

Eine Lösung dieser Probleme wäre mit einer komplett eigenständigen Signatur-Architektur möglich, d. h. mit einem speziellen System, das abgeschirmt von der Umgebung nur zur Überprüfung von Dateien vorgesehen ist. Da ein solches System jedoch einen eigenen Prozessor und eigene Peripheriegeräte wie Tastatur, Bildschirm, etc. benötigen würde, ist es für den vorgesehenen Zweck zu kostspielig.

Aus der US 5 406 624 ist eine Sicherheitsvorrichtung für einen Rechner bekannt, mit der sicherheitsrelevante Daten von dem möglicherweise mit Viren oder dergleichen infizierten Rechner ferngehalten werden. Die Vorrichtung dient ferner dazu, Vorgänge wie das Erzeugen von Schlüsseln und das Schreiben der Schlüssel auf Smart-Cards unabhängig von dem Rechner durchzuführen. Dazu ist der Rechner von seinen Peripheriegeräten isoliert, indem diese nicht direkt sondern über die zwischengeschaltete Sicherheitsvorrichtung mit dem Rechner verbunden sind. Zur Durchführung der sicherheitsrelevanten Vorgänge übernimmt die Vorrichtung die Kontrolle über die Peripheriegeräte und führt selbständig die erforderlichen Operationen wie etwa das Lesen oder Beschreiben einer Smart-Card durch. Die Sicherheitsvorrichtung ist jedoch nicht dafür geeignet, eine auf einem Ausgabegerät des Rechners ausgegebene, online empfangene oder zu versendende Datei auf deren Authentizität und Integrität zu überprüfen. Nachteilig an dieser Vorrichtung ist weiterhin, daß zu deren Aktivierung spezielle Befehle oder eine separate Switch-Box benötigt werden. Außerdem ist die Sicherheitsvorrichtung sehr aufwendig und damit teuer, da sie für die Durchführung komplexer Vorgänge, wie sie das Lesen und Beschreiben einer Smart-Card darstellen, ausgelegt ist. Zudem muß eine komplette, separate Bildschirmansteuerung in der Sicherheitsvorrichtung vorhanden sein.

Es ist daher Aufgabe der Erfindung, eine Möglichkeit zur Überprüfung einer empfangenen oder versandfertigen signierten Datei bereitzustellen, die eine möglichst sichere Information bezüglich der Authentizität und Integrität der auf einem Ausgabegerät eines Rechners ausgegebenen Datei liefert.

Gelöst wird diese Aufgabe durch ein Verfahren der eingangs genannten Art, bei dem zur Überprüfung auf Signale zugegriffen wird, die an einer Schnittstelle des Rechners zu einem Ausgabegerät für die Ausgabe der mit der digitalen Signatur versehenen Datei vorliegen. Dies ermöglicht eine Überprüfung der Daten, wie sie auf dem Ausgabegerät des Rechners ausgegeben und vom Benutzer wahrgenommen werden. Die Erfindung beruht auf der Erkenntnis, daß die Signale, die an ein Ausgabegerät des Rechners abgegeben werden, durch Viren oder dergleichen nicht angegriffen werden können, da das Ausgabegerät eine passive Einheit darstellt, die die Daten nicht mehr bearbeitet. Somit kann der Betrachter der signierten Datei darüber informiert werden, ob die auf dem Ausgabegerät ausgegebene Datei und die digitale Signatur zusammenpassen. Bei positivem Ergebnis ist auf diese Weise sichergestellt, daß die zur Überprüfung herangezogenen Daten (Datei und digitale Signatur) nicht nachträglich auf dem Rechner des Empfängers oder im Netzwerk manipuliert wurden.

Da vorgesehen ist, das erfindungsgemäße Verfahren in einer von der zentralen Recheneinheit (CPU) des Rechners logisch getrennten Vorrichtung durchzuführen, kann die Überprüfung der Datei nicht durch Viren oder dergleichen gestört werden, die möglicherweise auf die im Rechner stattfindende Datenverarbeitung einwirken.

Die Rekonstruktion der auf dem Ausgabegerät ausgegebenen Datei und deren digitaler Signatur aus den Signalen, die an der Schnittstelle vorliegen, ermöglicht eine verhältnismäßig unkomplizierte Überprüfung der ausgegebenen signierten Datei unter Verwendung bekannter Verfahren.

Vorzugsweise umfaßt das erfindungsgemäße Verfahren

die Entschlüsselung der digitalen Signatur der rekonstruierten signierten Datei, wobei durch die Entschlüsselung eine erste Digest-Zahl erzeugt wird. Diese erste Digest-Zahl kann dann auf einfache Weise mit einer zweiten Digest-Zahl verglichen werden, die aus der rekonstruierten Datei bestimmt wird. Das Ergebnis dieses Vergleichs gibt einen sicheren Aufschluß über die Authentizität und Integrität der ausgegebenen Datei, vorausgesetzt, daß der verwendete Schlüssel tatsächlich zum Absender gehört. Diese Zuordnung zwischen öffentlichem Schlüssel und Absender wird aber üblicherweise über eine unabhängige Zertifizierungsstelle sichergestellt. Zudem kann sich bei positivem Ergebnis des Vergleichs, wenn es sich bei der Datei um eine empfangene Datei handelt, der Empfänger sicher sein, daß die Datei vom Absender auch tatsächlich abgeschickt wurde. Somit kann z. B. der Absender ein in der Datei enthaltenes Angebot nicht gegenstandslos machen, indem er bestreitet, diese Datei jemals abgeschickt zu haben.

Gemäß einer Weiterbildung des Verfahrens ist Vorgesehen, auch den Erstellungszeitpunkts der mit der digitalen Signatur versehenen Datei zu überprüfen. So kann z. B. bei empfangenen Dateien eine gesicherte Auskunft über die Gültigkeit eines in der signierten Datei enthaltenen, zeitlich befristeten Angebots zum Zeitpunkt des Empfangs gegeben werden.

Besonders geeignet ist das erfindungsgemäße Verfahren für Dateien, die online aus einem Netzwerk empfangen wurden bzw. online über ein Netzwerk versendet werden, da solche Dateien einem erhöhten Risiko der fehlerhaften Übertragung oder Manipulation unterliegen.

Schließlich erweist es sich als vorteilhaft, wenigstens einen Teil des Verfahrens mittels einer Chipkarte durchzuführen. Wenn der Rechner beispielsweise mit einem Smart-Card-Terminal ausgestattet ist, können mit einer entsprechenden Smart-Card sowohl im Zusammenhang mit dem erfindungsgemäßen Verfahren erforderliche Entschlüsselungsvorgänge als auch Überprüfungen von Schlüsseln unterstützt werden.

Die Erfindung sieht auch eine Vorrichtung zur Durchführung des Verfahrens vor, die eine Schaltung und ein Programm umfaßt, mit denen in der Vorrichtung und logisch getrennt von der zentralen Recheneinheit des Rechners die Überprüfung durchgeführt wird, wobei die Vorrichtung mit einer Schnittstelle des Rechners zu einem Ausgabegerät so gekoppelt ist, daß sie die für die Überprüfung verwendeten Signale zur Ausgabe der mit der digitalen Signatur versehenen Datei erfaßt. Mit der erfindungsgemäßen Vorrichtung können so auf einfache Weise die für die Ausgabe der signierten Datei vorgesehenen, nicht angreifbaren Signale abgetastet und ausgewertet werden. Auch die Überprüfung der Datei kann aufgrund der Trennung der Vorrichtung von der Datenverarbeitung des Rechners nicht gestört werden.

Vorzugsweise ist die Vorrichtung an die Schnittstelle des Rechners zu einem Bildschirm gekoppelt. So erhält beispielsweise der Empfänger einer Datei die gesicherte Information, ob die empfangene Datei in der Form, wie sie am Bildschirm angezeigt wird, tatsächlich vom angegebenen Absender stammt und störungsfrei übertragen wurde. Die Vorrichtung kann jedoch auch an die Schnittstelle des Rechners zu einem Drucker gekoppelt sein.

Für eine kostengünstige Herstellung der Vorrichtung ist es vorteilhaft, daß die Vorrichtung einen ASIC (application-specific integrated circuit) umfaßt, der die für die Überprüfung notwendige Schaltung beherbergt. Der ASIC kann auch einen Mikroprozessor aufweisen, der programmgesteuert arbeitet.

Eine Flexibilität in bezug auf die Auswahl des Rechners, an dem die Vorrichtung eingesetzt werden soll, wird dadurch erreicht, daß die Vorrichtung für die nachträgliche Ausstattung des Rechners geeignet ist, d. h. als sogenanntes Add-On-System ausgeführt ist. Die Vorrichtung kann auf einfache Weise an dem gewünschten Rechner eingerichtet und bei Bedarf wieder deinstalliert werden, um einen anderen Rechner mit der Vorrichtung auszustatten.

Die Vorrichtung kann intern auf der Basisplatine (motherboard) oder auf einer Einsteckkarte des Rechners angeordnet sein. Sie kann aber auch in einem externen Gerät verwirklicht sein, das an den Rechner angeschlossen ist. So ist es beispielsweise möglich, die Vorrichtung in ein Chipkarten-Terminal, z. B. ein Smart-Card-Lese-/Schreibgerät zu integrieren. Vorzugsweise weist die Vorrichtung eine dem Chipkarten-Terminal zugeordnete Chipkarte auf, die so mit der restlichen Vorrichtung verknüpft ist, daß sie einen Entschlüsselungsvorgang zumindest teilweise durchführt oder Daten für einen Entschlüsselungsvorgang bereitstellt. Somit besteht die Möglichkeit, wenigstens einen Teil des erfindungsgemäßen Verfahrens mit Hilfe oder direkt von einem Mikroprozessor der Smart-Card durchführen zu lassen. Mit dem Terminal können aber auch andere, auf das erfindungsgemäße Verfahren bezogene Funktionen ausgeführt werden.

Um den Benutzer einfach und unkompliziert über das Ergebnis der Dateiüberprüfung zu informieren, umfaßt die Vorrichtung eine TRUE/FALSE-Anzeige.

Eine bevorzugte Ausführungsform der erfindungsgemäßen Vorrichtung umfaßt eine Echtzeituhr, mit deren Hilfe das Alter einer signierten Datei bestimmt werden kann. Dies kann z. B. für die Überprüfung erforderlich sein, ob ein in der Datei enthaltenes Angebot noch gültig ist.

Falls die Vorrichtung an wechselnden Orten aufgestellt werden soll, kann die Kopplung der Vorrichtung an die Schnittstelle des Rechners drahtlos erfolgen. Damit ist die Auswahl der Standorte nicht durch die Länge eines Kabels oder dessen unerwünschte Sichtbarkeit beeinträchtigt.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden beispielhaften Beschreibung unter Bezugnahme auf die Zeichnung. In dieser zeigen:

Fig. 1 ein schematisches Flußdiagramm für die Verarbeitung einer zu versendenden Datei; und

Fig. 2 ein schematisches Flußdiagramm für die Überprüfung einer empfangenen Datei mit der erfindungsgemäßen Vorrichtung, die nach dem erfindungsgemäßen Verfahren arbeitet.

Im folgenden werden das erfindungsgemäße Verfahren und die dafür vorgesehene erfindungsgemäße Vorrichtung am Beispiel der Überprüfung einer empfangenen Datei beschrieben. Es ist jedoch genauso möglich, das Verfahren und die Vorrichtung auf der Seite des Empfängers zur Überprüfung einer versandfertigen Datei, die an der Schnittstelle zum Netzwerk anliegt, zu verwenden.

In **Fig. 1** sind die Vorgänge dargestellt, der gemäß dem Konzept der Public-Key-Kryptographie üblicherweise auf einem Rechner **10** des Absenders vor dem Versenden einer Datei ablaufen. Aus der von dem Absender erstellten Datei, die zu einem Empfänger geschickt werden soll, wird mittels eines vorgegebenen mathematischen Algorithmus eine sogenannte Digest-Zahl berechnet. Eine Digest-Zahl hat eine bestimmte Länge und ist für die jeweilige Datei spezifisch, d. h. die kleinste Änderung in der Datei würde zu einem unterschiedlichen Wert führen. Andererseits kann jedoch aus der Digest-Zahl niemals die ursprüngliche Datei erhalten werden. Die Digest-Zahl der Datei wird mittels eines privaten Schlüssels (private key) des Absenders verschlüsselt, der nur dem Absender bekannt ist. Das Ergebnis dieser Verschlüsselung wird als digitale Signatur der Datei bezeichnet. Die digitale Signatur wird an die zu versendende Datei angehängt. Die mit der digitalen Signatur verschene (signierte)

Datei kann nun entweder gleich über ein Netzwerk **12** an den Empfänger verschickt oder, falls die Daten vertraulich sind, vorher verschlüsselt werden.

Die optionale Verschlüsselung der signierten Datei erfolgt üblicherweise mittels eines zufällig erzeugten einmaligen Schlüssels (one time key). Der einmalige Schlüssel selbst wird wiederum mit einem öffentlichen Schlüssel (public key) verschlüsselt und anschließend an die signierte, verschlüsselte Datei angehängt. Beide zusammen werden schließlich als "gesicherte Datei" an den Empfänger verschickt.

Fig. 2 zeigt die Vorgänge, die zur Überprüfung der empfangenen Datei auf der Seite des Empfängers durchgeführt werden. Die von einem Rechner **14** empfangene Datei wird als gesicherte oder lediglich signierte Datei erkannt. Im ersten Fall wird die gesicherte Datei zunächst auf dem Rechner **14** mittels eines privaten Schlüssels des Empfängers entschlüsselt, wodurch eine signierte, aber noch verschlüsselte Datei und ein einmaliger Schlüssel erhalten werden. Mit dem einmaligen Schlüssel kann nun die signierte, verschlüsselte Datei entschlüsselt werden. Die daraus resultierende signierte Datei wird anschließend so weiterverarbeitet wie eine unverschlüsselt empfangene Datei, die mit einer Signatur versehen ist.

Um die signierte Datei für den Empfänger sichtbar zu machen, wird sie auf einem Ausgabegerät **16** ausgegeben, das über eine Schnittstelle **18** an den Rechner **14** angeschlossen ist. Das Ausgabegerät **16** ist im Regelfall ein Bildschirm, es kann jedoch beispielsweise auch ein Drucker o. ä. vorgesehen sein. Die vom Rechner **14** an das Ausgabegerät **16** abgegebenen Signale zur Anzeige der signierten Datei sind logisch von der zentralen Recheneinheit des Rechners **14** getrennt, d. h. diese Signale können nicht durch Programme beeinflußt werden, die auf dem Rechner **14** ablaufen. Somit sind diese Signale auch nicht durch Viren oder dergleichen angreifbar.

An der Schnittstelle **18** ist neben dem Ausgabegerät **16** auch eine Vorrichtung **20** angeschlossen, die auf die für das Ausgabegerät **16** bestimmten Signale zugreifen kann. Normalerweise handelt es sich bei einer Schnittstelle **18** zu einem Bildschirm um eine analoge Schnittstelle. Bei modernen Bildschirmen, die die anzuzeigenden Daten selbst in analoge Signale umwandeln, ist dementsprechend eine digitale Schnittstelle vorgesehen. Der Einfachheit halber werden die in diesem Fall an der Schnittstelle vorliegenden Daten ebenfalls als "Signale" bezeichnet. Sowohl die Verbindung des Ausgabegeräts **16** als auch der Vorrichtung **20** mit der Schnittstelle **18** des Rechners **14** kann drahtlos erfolgen, z. B. mittels aufeinander abgestimmter Infrarot-Schnittstellen an den beteiligten Geräten.

Die Vorrichtung **20** weist eine elektronische Schaltung, die in einem ASIC untergebracht sein kann, und ein geeignetes Programm zur Überprüfung der signierten Datei auf. Da die Vorrichtung **20** logisch getrennt von der zentralen Recheneinheit des Rechners **14** ist, können keine Viren oder dergleichen, die sich beispielsweise im Hauptspeicher des Rechners **14** befinden und die Datenverarbeitung auf unerwünschte Weise beeinflussen, die Überprüfung der signierten Datei stören.

Die Überprüfung der signierten Datei in der Vorrichtung **20** wird im folgenden für den Fall eines Bildschirms als Ausgabegerät **16** beschrieben: Die an der Schnittstelle **18** vorliegenden Signale werden von der Vorrichtung **20** abgetastet und ausgewertet. Dadurch kann das auf dem Bildschirm ausgegebene Bild rekonstruiert werden, und die darin "angezeigte" Datei samt zugehöriger digitaler Signatur wird ausfindig gemacht. Die digitale Signatur wird mittels eines öffentlichen Schlüssels entschlüsselt, der vom Absender öffentlich zugänglich gemacht wurde und auf den privaten Schlüssel abgestimmt ist, mit dem die vom Absender aus der ursprünglichen Datei erzeugte Digest-Zahl verschlüsselt wurde. Der öffentliche Schlüssel ist von einer unabhängigen Zertifizierungsstelle zertifiziert. Das Ergebnis dieser Entschlüsselung ist eine erste Digest-Zahl. Eine zweite Digest-Zahl wird aus der Datei selbst berechnet. Dazu wird der gleiche mathematische Algorithmus verwendet, der auf dem Rechner **10** des Absenders die ursprüngliche Digest-Zahl erzeugt hat. Die für diesen Vorgang notwendigen Informationen über den mathematischen Algorithmus sind mit der digitalen Signatur verschickt worden. Die beiden Digest-Zahlen werden schließlich miteinander verglichen und das Ergebnis wird über eine TRUE/FALSE-Ausgabeeinrichtung **22** der Vorrichtung **20** ausgegeben. Das Ergebnis kann beispielsweise bei übereinstimmenden Digest-Zahlen (TRUE) durch eine grüne Leuchtdiode und bei nicht übereinstimmenden Digest-Zahlen (FALSE) durch eine rote Leuchtdiode angezeigt werden.

Stimmen die beiden Digest-Zahlen überein, wurde die Datei nach dem Signieren durch den Absender nicht mehr verändert. Außerdem hat der Empfänger hat Gewißheit über die Identität des Absenders, da durch die Zertifizierung des öffentlichen Schlüssels dessen Zugehörigkeit zu dem Absender sichergestellt ist. Da alleine der Absender Zugriff auf den privaten Schlüssel hat, der zum Signieren der Datei benutzt wurde, kann der Absender auch nicht abstreiten, daß er die Datei verschickt hat. Bei Nichtübereinstimmung der beiden Digest-Zahlen muß davon ausgegangen werden, daß die Datei entweder nicht korrekt übertragen oder manipuliert wurde oder daß die Signatur mit einem privaten Schlüssel erzeugt wurde, der nicht zu dem für die Entschlüsselung der digitalen Signatur benutzten öffentlichen Schlüssel paßt.

Eine bevorzugte Ausführungsform der Vorrichtung **20** umfaßt zusätzlich eine Echtzeituhr **24** zur gesicherten Bestimmung des Alters der Datei, z. B. der Zeitdifferenz zwischen Empfangs- und Erstellungszeitpunkt der Datei. Dazu wird die Datei vor dem Verschicken neben der digitalen Signatur mit einer Angabe über den Erstellungs- oder Absendezeitpunkt oder den Gültigkeitszeitraum versehen, die als Zeitstempel bezeichnet werden kann. In der Vorrichtung **20** kann nun anhand eines Vergleichs dieser Zeitangabe mit der aktuellen Zeit ermittelt werden, ob z. B. ein in der Datei enthaltenes, zeitlich befristetes Angebot noch gültig ist. Diese Überprüfung wird dann bei der Anzeige des Ergebnisses der Dateiüberprüfung mit berücksichtigt.

Die Vorrichtung **20** ist als Add-On-System konzipiert, d. h. ein Rechner kann nachträglich mit der Vorrichtung **20** ausgestattet werden. Dabei kann die Vorrichtung **20** sowohl intern im Rechner **14** auf der Basisplatine oder auf einer Einsteckkarte angeordnet sein. Gemäß einer weiteren Ausführungsform ist die die Vorrichtung **20** in ein Smart-Card-Terminal integriert. Mit Hilfe des Smart-Card-Terminals und entsprechender Smart-Card kann gleichzeitig die Zertifizierung des öffentlichen Schlüssels überprüft werden, der für die Entschlüsselung der digitalen Signatur benötigt wird. Weiterhin kann mit Hilfe einer geeigneten Smart-Card die Entschlüsselung der digitalen Signatur oder gegebenenfalls der gesicherten Datei unterstützt werden. Die Smart-Card enthält beispielsweise einen für die jeweilige Entschlüsselung notwendigen Schlüssel und/oder ein Entschlüsselungsprogramm. Ein Teil oder die gesamte Entschlüsselung kann von einem Mikroprozessor der Smart-Card durchgeführt oder gesteuert werden.

Patentansprüche

1. Verfahren zur Überprüfung der Authentizität und

Integrität einer von einem Rechner (10; 14) empfangenen oder zu versendenden Datei, die mit einer digitalen Signatur versehen ist, **dadurch gekennzeichnet**, daß zur Überprüfung auf Signale zugegriffen wird, die an einer Schnittstelle (18) des Rechners (10; 14) zu einem Ausgabegerät (16) für die Ausgabe der mit der digitalen Signatur versehenen Datei vorliegen.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Verfahren in einer von der zentralen Recheneinheit des Rechners (10; 14) logisch getrennten Vorrichtung (20) durchgeführt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Verfahren die Rekonstruktion der auf dem Ausgabegerät (16) ausgegebenen, mit der digitalen Signatur versehenen Datei aus den Signalen umfaßt, die an der Schnittstelle vorliegen.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß das Verfahren die Entschlüsselung der digitalen Signatur der rekonstruierten signierten Datei umfaßt, wobei durch die Entschlüsselung eine erste Digest-Zahl erzeugt wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß das Verfahren die Bestimmung einer zweiten Digest-Zahl aus der rekonstruierten Datei und das Vergleichen der ersten Digest-Zahl mit der zweiten Digest-Zahl umfaßt.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Verfahren die Überprüfung des Erstellungszeitpunkts der mit der digitalen Signatur versehenen Datei umfaßt.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die mit der digitalen Signatur versehene Datei online aus einem Netzwerk empfangen wurde bzw. online über ein Netzwerk versendet wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß wenigstens ein Teil des Verfahrens mittels einer Chipkarte durchgeführt wird.

9. Vorrichtung zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Vorrichtung (20) eine Schaltung und ein Programm umfaßt, mit denen in der Vorrichtung (20) und logisch getrennt von der zentralen Recheneinheit des Rechners (10; 14) die Überprüfung durchgeführt wird, und die Vorrichtung (20) mit einer Schnittstelle (18) des Rechners (10; 14) zu einem Ausgabegerät (16) so gekoppelt ist, daß sie die für die Überprüfung verwendeten Signale zur Ausgabe der mit der digitalen Signatur versehenen Datei erfaßt.

10. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Vorrichtung (20) an die Schnittstelle (18) des Rechners (10; 14) zu einem Bildschirm gekoppelt ist.

11. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Vorrichtung (20) an die Schnittstelle (18) des Rechners (10; 14) zu einem Drucker gekoppelt ist.

12. Vorrichtung nach einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, daß die Vorrichtung (20) einen ASIC umfaßt.

13. Vorrichtung nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, daß die Vorrichtung (20) für die nachträgliche Ausstattung des Rechners (10; 14) geeignet ist.

14. Vorrichtung nach einem der Ansprüche 9 bis 13, dadurch gekennzeichnet, daß die Vorrichtung (20) auf der Basisplatine des Rechners (10; 14) angeordnet ist.

15. Vorrichtung nach einem der Ansprüche 9 bis 13, dadurch gekennzeichent, daß die Vorrichtung (20) auf einer Einsteckkarte des Rechners (10; 14) angeordnet ist,

16. Vorrichtung nach einem der Ansprüche 9 bis 13, dadurch gekennzeichnet, daß die Vorrichtung (20) in ein Chipkarten-Terminal integriert ist.

17. Vorrichtung nach Anspruch 16, dadurch gekennzeichnet, daß die Vorrichtung (20) eine dem Chipkarten-Terminal zugeordnete Chipkarte aufweist, die so mit der restlichen Vorrichtung verknüpft ist, daß sie einen Entschlüsselungsvorgang zumindest teilweise durchführt oder Daten für einen Entschlüsselungsvorgang bereitstellt.

18. Vorrichtung nach einem der Ansprüche 9 bis 17, dadurch gekennzeichnet, daß die Vorrichtung (20) eine TRUE/FALSE-Anzeigeeinrichtung umfaßt.

19. Vorrichtung nach einem der Ansprüche 9 bis 18, dadurch gekennzeichnet, daß die Vorrichtung (20) eine Echtzeituhr (22) umfaßt.

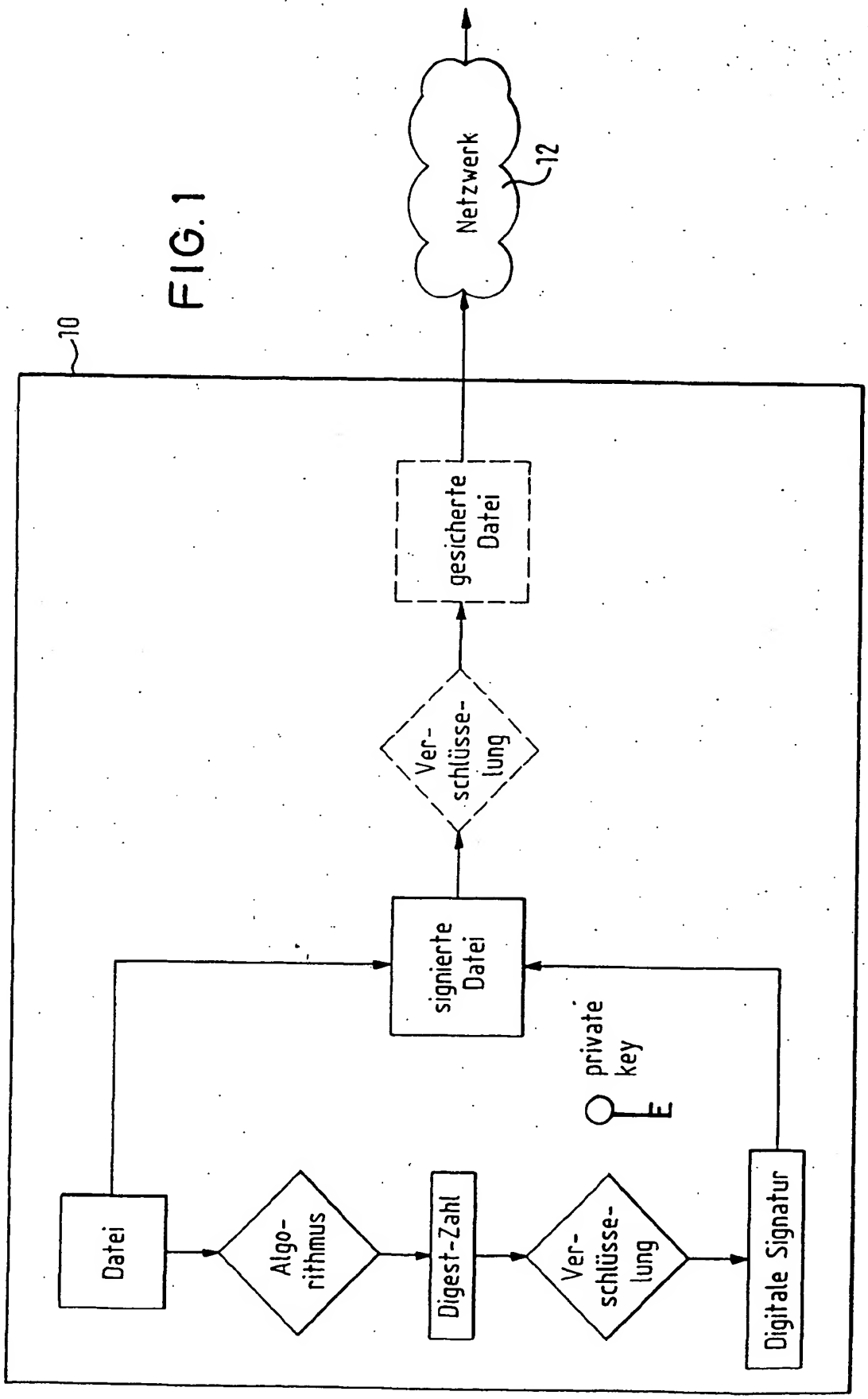
20. Vorrichtung nach einem der Ansprüche 9 bis 19, dadurch gekennzeichnet, daß die Kopplung der Vorrichtung (20) an die Schnittstelle (18) des Rechners (10; 14) drahtlos erfolgt.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 199 61 838 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 5. Juli 2001

FIG. 1



Nummer: DE 199 61 838 A1
Int. Cl.[7]: H04L 9/32
Offenlegungstag: 5. Juli 2001

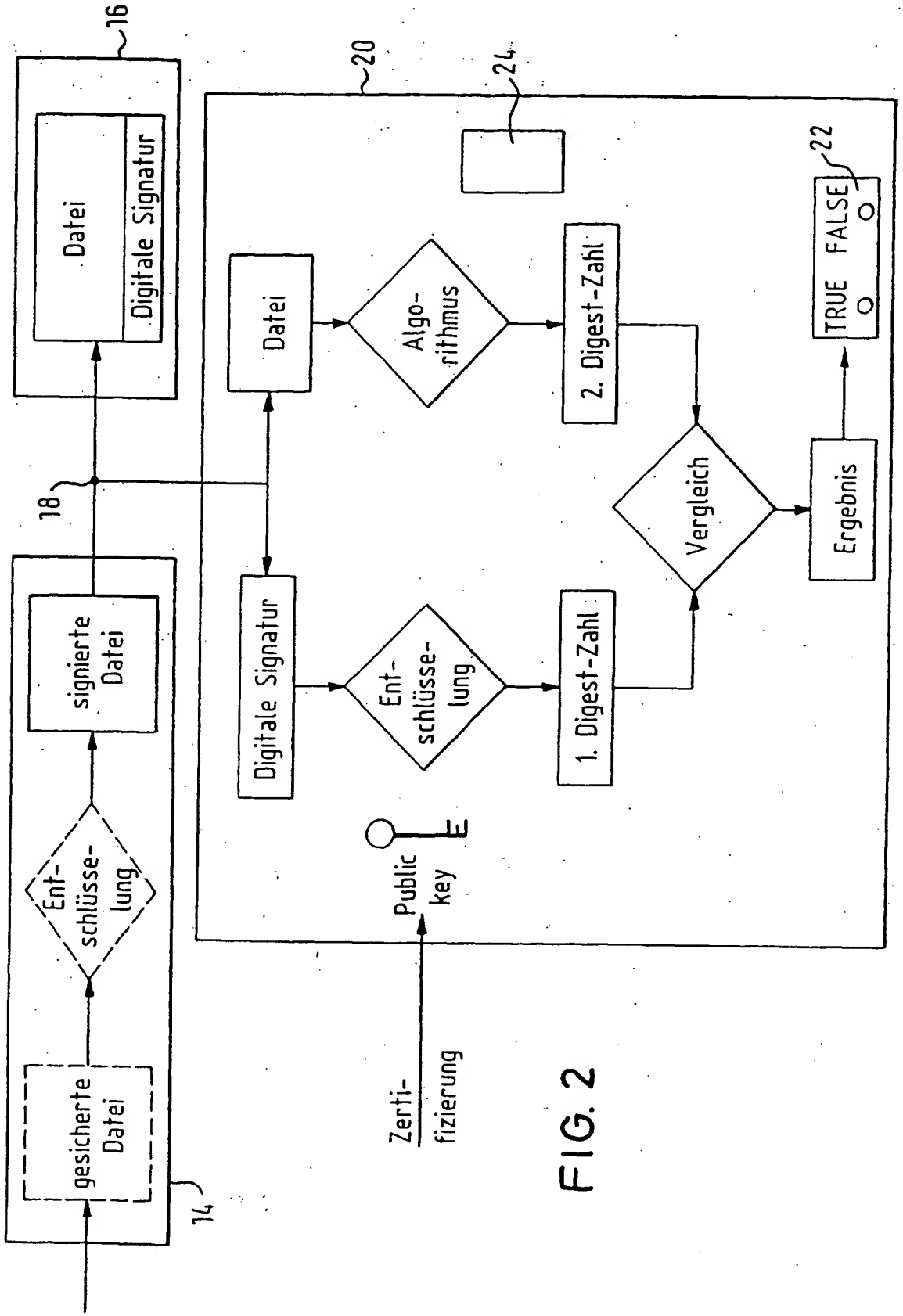


FIG. 2